

ANSI C12.22, IEC 1703, MC 12.22 Tutorial

Edward J. Beroaset
17 May 2010



ANSI C12.19



- “The ANSI C12.19 standard provides a common data structure for use in transferring data to and from utility end devices, typically meters.”
- from ANSI C12.19-1997 Foreword
- Provides data structures but *not* protocol
- Includes explicit provisions for manufacturer innovation by inclusion of Manufacturer’s Tables

ANSI Communication Protocols



- ANSI C12.18-1996 (2006)
 - optical port communications
- ANSI C12.21-1999 (2006)
 - telephone modem communications
- ANSI C12.22-2008
 - data network
- Each works with ANSI C12.19 (the tables)

Overview



- Prehistoric times
- Early ANSI
- ANSI C12.19
- ANSI C12.18
- ANSI C12.21
- ANSI C12.22
- Security aspects
- A Sample

C12.18 Review



- Simple optical port protocol
- Point-to-point communication
- Medium error rate, low latency link assumed
- Close physical proximity
- Half duplex (TX or RX -- never both)
- Defines and uses PSEM (Protocol Specification for Electric Metering)
- Also defines physical attributes of port

PSEM Services in C12.18



- Identification – what kind of device is this?
- Read – get table data
- Write – send table data
- Logon – establish the basic logical link
- Security – send a password
- Logoff – gracefully terminate logical link
- Negotiate – change link speed, other parameters
- Wait – hold the link open while processing
- Terminate – immediately end communications

C12.21 Additions



- Minimal adaptation of C12.18 to modem
 - Added PSEM services:
 - Timing Setup
 - Authenticate
 - Disconnect
 - Modified some existing PSEM services:
 - Identification
 - Logoff
 - Terminate
- Minimal adaptation of C12.19 to modem
 - Added Decade 9 - Telephone Control tables

C12.22



- Title is “Protocol Specification for Interfacing to Data Communication Networks”
- Defines EPSEM (Extended PSEM)
- Defines an application layer protocol that may be used over a variety of underlying transports
- Adds robust security model incorporating authentication and encryption
- Useful for TCP/IP connected devices
- Used over IPv4 or IPv6
- Doesn't require IP

Why C12.22?



- Different purposes, different environments
- C12.21 and C12.18 assumptions:
 - point-to-point link
 - Low latency
 - moderate to high error rates
 - Must specify lower layers
- C12.22 assumptions
 - Network of connections
 - Possibly high latency
 - Low *effective* error rates
 - Cannot specify lower layers

Condition/Response in C12.22



- Network of connections
 - Addressing must be possible among large numbers of nodes
 - Routing and forwarding functions defined
- Possibly high latency
 - Connectionless mode defined
 - Request/response aggregation supported
- Low *effective* error rates
 - No further CRC required
- Cannot specify lower layers
 - Accommodates Ethernet, WiFi, RS-232, carrier pigeon

C12.22 Security



- Uses AES-128 in CBC and CTR modes
- Provides for Authenticated Encryption with Associated Data (AEAD) using a mode called EAX'
- Features
 - Data is encrypted (using AES-128)
 - both encrypted data and unencrypted header are authenticated (e.g. can't be altered without detection)
 - usable for both session and sessionless communication

A Sample



- 0000 00 50 59 85 19 c2 00 1e ec 30 94 74 08 00 45 00
- 0010 00 a8 eb 0d 40 00 80 06 73 aa 0a 02 a7 32 42 20
- 0020 a8 43 05 7d 04 81 c3 6a 5d 73 0b 08 e0 01 80 18
- 0030 ff ff e5 8a 00 00 01 01 08 0a 00 03 10 00 01 db
- 0040 dc 96 60 72 a2 11 06 0f 2b 06 01 04 01 82 85 63
- 0050 8e 7f 85 f1 c2 4e 01 a6 09 06 07 2b 06 01 04 82
- 0060 85 63 a8 06 02 04 2b c8 1a a1 ac 0f a2 0d a0 0b
- 0070 a1 09 80 01 00 81 04 4b 97 d2 cc be 39 28 37 81
- 0080 35 88 be b0 98 9f ad b0 20 eb 72 ba 46 35 3c c0
- 0090 a2 ac 2a 00 7a 10 1a fe ba f9 68 0d 3b 96 59 f9
- 00a0 91 12 1b 86 5f 25 4f 6a c9 2c dd 21 3d 31 e3 c4
- 00b0 d2 ca e6 f8 9b 6d

A sample PDU



- C1222-MESSAGE
 - called-AP-title: 1.3.6.1.4.1.33507.1919.12345678.1
 - calling-AP-title: 1.3.6.1.4.33507
 - calling-AP-invocation-id: 734534305
 - calling-authentication-value
 - calling-authentication-value-encoding: calling-authentication-value-single-asn1 (0)
 - calling-authentication-value-single-asn1: calling-authentication-value-c1222 (1)
 - calling-authentication-value-c1222
 - key-id-element: 00
 - iv-element: 4b97d2cc

User-information



- user-information
- C12.22 EPSEM Flags: 0x88
- 1... = C12.22 Reserved Flag: True
- .0.. = C12.22 Recovery Flag: False
- ..0. = C12.22 Proxy Service Used Flag: False
- ...0 = C12.22 ED Class Flag: False
- 10.. = C12.22 Security Mode Flags: Ciphertext with authentication (0x02)
-00 = C12.22 Response Control Flags: Always respond (0x00)
- [... 52 bytes of encrypted data ...]
- C12.22 EPSEM MAC: e6f89b6d

Questions?



If you think of questions later, you may contact me:

Ed Beroset

Director of Technology and Standards

Elster Solutions, LLC

email: edward.j.beroset@us.elster.com

office: 919-250-5424